Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore Maya (SBN 223242)
tmaya@ahdootwolfson.com
Bradley K. King (SBN 274399)
bking@ahdootwolfson.com
Christopher Stiner (SBN 276033)
cstiner@ahdootwolfson.com
Rachel Johnson (SBN 331351)
rjohnson@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, California 91505
Tel: (310) 474-9111
Fax: (310) 474-8585

Mark C. Molumphy (SBN 168009)
mmolumphy@cpmlegal.com
Joseph W. Cotchett (SBN 36324)
jcotchett@cpmlegal.com
Tyson Redenbarger (SBN 294424)
tredenbarger@cpmlegal.com
Noorjahan Rahman (SBN 330572)
nrahman@cpmlegal.com
Julia Peng (SBN 318396)
jpeng@cpmlegal.com
COTCHETT, PITRE & McCARTHY LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: 650.697.6000
Facsimile: 650.697.0577

Interim Co-Lead Class Counsel

COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
TRAVIS LEBLANC (251097)
(tleblanc@cooley.com)
KATHLEEN R. HARTNETT (314267)
(khartnett@cooley.com)
BENJAMIN H. KLEINE (257225)
(bkleine@cooley.com)
DANIELLE C. PIERRE (300567)
(dpierre@cooley.com)
JOSEPH D. MORNIN (307766)
(jmornin@cooley.com)
EVAN G. SLOVAK (319409)
(eslovak@cooley.com)
KELSEY R. SPECTOR (321488)
(kspector@cooley.com)
101 California Street, 5th Floor
San Francisco, California 94111-5800
Telephone: +1 415 693 2000
Facsimile: +1 415 693 2222

Attorneys for Defendant
ZOOM VIDEO
COMMUNICATIONS, INC.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: ZOOM VIDEO COMMUNICATIONS, INC. PRIVACY LITIGATION

This Document Relates To: All Actions

Case No. 5:20-CV-02155-LHK

SUPPLEMENTAL JOINT STATEMENT REGARDING DISCOVERY DISPUTE

Magistrate Susan van Keulen, presiding

Following the Court's February 16, 2020 Order (Dkt 154), the Parties met and conferred and resolved all issues, except the discrete issues described below.

I. PLAINTIFFS' POSITION

Third Party Applications:

Surreptitious information collecting is a core issue in Plaintiffs' case. On Zoom's platform, Marketplace apps alike allow for personal information collection without the user's awareness. Additionally, app developers pay Zoom for access to user information via the MarketPlace. Discovery on a limited number of apps is therefore proportional and relevant in this case.

In an effort to compromise, and in accordance with the discussion with the Court, Plaintiffs proposed narrowing both the number of apps and the number of Requests for Production ("RFPs") as follows:

a. Plaintiffs agreed to limit the requests at issue to RFPs 13, 22, 24, 35, 53, 54, and 57.

b. With regard to those requests, Plaintiffs will identify, by February 21, 2021, 10 specific apps from Zoom's Marketplace for Zoom to include in its search for responsive data. Plaintiffs will identify these apps by looking at the number and types of permissions, whether the host or user runs the app, and the volume of API traffic.

This proposal is both considerably more narrow and tailored than Plaintiffs' prior proposal and is reasonable given the nature of the claims in this case. Zoom rejected this offer and provided no counter offer. The Court should adopt Plaintiffs' proposal on the third party apps as it relates to RFPs 13, 22, 24, 35, 53, 54, and 57.

Encryption Search Terms:

Regarding the Court's order that the parties continue meeting and conferring on search terms related to encryption-based claims, Plaintiffs proposed the search terms shown in the table below as compromise, search terms (in addition to those Zoom already is using). Zoom then provided the following hit counts to Plaintiffs:

///

Terms	Documents with hits, including family	Unique hits
"green lock"	254	32
"green shield"	124	36
Stor* w/3 key*	65,767	7,671
AES w/10 meeting	7,674	941
(ECB or CBC or CBC-MAC or GCM or OFM or CBC) w/10 meeting	7,823	1,395
(encipher or decipher or decrypt) w/10 meeting	17,867	1,487

Plaintiffs' proposed search term of "Stor* w/3 key*" is narrowly tailored to return documents concerning the storage of encryption keys, which is a critical issue in this case. This term resulted in only 7,671 unique hits on Zoom's hit report, which is not burdensome and, therefore, Plaintiffs do not agree to limit this term. As a counter, Zoom proposed running "(stor* w/3 key*) w/10 meeting," and in exchange, offered to run "AES w/10 meeting." That is not a compromise. Plaintiffs proposed "AES w/10 meeting" as a separate term, which is also very relevant as AES describes the specific type of encryption at issue in this case. "AES w/10 meeting" only returned 941 unique hits, thus production on that search term is not burdensome. Accordingly, Zoom's proposal to limit "Stor* w/3 key*" and to potentially not run "AES w/10 meeting" is not acceptable.

Plaintiffs respectfully request that the Court order Zoom to run all of Plaintiffs' proposed compromise search terms. They both address highly important issues in this case (including encryption algorithms that are not end-to-end and methods of their use), and do not result in unduly burdensome, unique hit counts. In addition, Zoom can reduce any burden by doing a targeted privilege review (e.g., by searching for key terms: attorney names, domain names of firms), and producing the rest of the hits to us, subject to the FRE 502 Order and agreement in place (Dkt. 140).

Lastly, Zoom indicated that it would do a relevance review of the encryption documents – plaintiffs object to any type of relevance review. If non-privileged documents were located based on any of the proposed search terms, those should be produced.

II. ZOOM'S POSITION

Marketplace Apps. Zoom has met and conferred in good faith with Plaintiffs on the issue

of Marketplace Apps and respectfully submits that Plaintiffs still have failed to substantiate their position that additional discovery into Marketplace Apps is relevant to this matter or proportionate. Even narrowed discovery remains unwarranted absent a showing of relevance or reasonable investigation to support the request. Therefore, the requested discovery should be denied.

In response to the Court's February 16, 2021 Order, Plaintiffs now propose discovery into fewer Marketplace Apps (10) with respect to fewer Requests for Production ("RFPs") (7). But they still have failed to identify any specific Marketplace App for which they will seek discovery, despite Zoom's request. Indeed, Plaintiffs' reductions are entirely arbitrary. They are not due to any relevance of the reduced subset of RFPs—or the relevance of any specific Marketplace App they might eventually pick—to this case. Simply reducing the amount of irrelevant discovery sought does not make the discovery any more relevant or appropriate.

As Zoom explained at the hearing earlier this week, Plaintiffs are putting the cart before the horse by seeking discovery into unidentified Marketplace Apps not at issue in this lawsuit before doing any investigation whatsoever into these Apps. Information about Zoom's Marketplace Apps is publicly available, and yet Plaintiffs have provided no basis for discovery into any of these Apps other than LinkedIn Sales Navigator (which they have pleaded in their First Amended Complaint, although they have failed to connect it to any Plaintiff's experience) and Marketo (which is irrelevant but which Zoom agreed to give discovery on because it is the one Marketplace App with a "security advisory"—notably, about the Marketo software, not about Zoom's). As Plaintiffs conceded at this week's hearing, they could have their experts run testing to determine whether any Marketplace App presents a privacy issue, but they have not. Plaintiffs argue that the cost is prohibitive (Plaintiffs' counsel stated at the hearing that it would cost $5 million to test all Apps in the Marketplace—i.e., a cost per app of approximately $4,500). But just because it would cost money for Plaintiffs to investigate issues before seeking discovery in no way justifies shifting the burden to Zoom to produce documents unjustified by any allegation or argument. Plaintiffs' attempt to shift the cost of their fishing expedition to Zoom is inappropriate and should be rejected.

Notably, even now, in the face of the Court's February 16, 2021 Order, Plaintiffs refuse to specify which additional Marketplace Apps they seek to investigate. Instead, they say that their 10

unilaterally chosen "apps will be identified by looking at number and types of permissions, whether host or user runs the app, and volume of API traffic," but these are all inquiries that Plaintiffs could have and should have made—in order to determine if there is any relevance whatsoever to this case—before going down the road to requesting this irrelevant discovery. Zoom cannot assess relevance and burden if Plaintiffs refuse to disclose the Apps they will seek discovery on. In contrast, Zoom has agreed to produce information regarding SDKs as reflected in the Court's order.

Moreover, although Plaintiffs have arbitrarily reduced the number of proposed RFPs for which they seek Marketplace App-related discovery (namely, RFPs 13, 22, 24, 24, 35, 53, 54, 57), these RFPs still seek an unjustifiably wide and burdensome swath of information—unlike a more narrow topic such as "security audit information," as suggested by the Court's Order. Specifically, Plaintiffs seek irrelevant and disproportionate discovery into Zoom's network security (RFP 13); general security assessments (RFP 22); usership statistics (RFP 24); government investigations (RFP 35); the design of Zoom's networks and information systems (RFPs 53, 54); and data traffic-related procedures (57). These requests are unjustified and should be denied.

End-to-End Encryption. As an initial matter, Plaintiffs' premise for adding to Zoom's proposed end-to-end encryption-related search terms is incorrect. Plaintiffs have alleged in this case that the end-to-end encryption implementation Zoom had in place prior to April 2020 was not actually end-to-end encryption (which Zoom disputes), and thus they contend that "end-to-end"-based search terms are insufficient regarding the earlier implementation. This is incorrect. Based on diligent investigation, Zoom proposed search terms to hit on documents related to Zoom's implementation of encryption for Zoom Meetings videoconferences throughout the entire class period. Given that Zoom's position is that it did have end-to-end encryption, it is not surprising that Zoom's documents would refer to its encryption implementation using "end-to-end"-based language.

Specifically, Zoom's terms (end-to-end w/3 encryption, E2EE, E2E, and ETEE) hit on approximately 125,431 documents plus families for Zoom custodians between 3/30/16 and 4/30/20 that Zoom has agreed to review. Any discussion of additional terms must acknowledge that Zoom's proposed terms were designed to hit on a large number of documents for the entire class period.

During the parties' meet and confer yesterday, Plaintiffs proposed the following search terms, which Zoom agreed to consider depending on search term hits – hit counts are shown below:

	Terms	Documents, including family	Unique hits
1	"green lock"	254	32
2	"green shield"	124	36
3	Stor* w/3 key*	65,767	7,671
4	AES w/10 meeting	7,674	941
5	(ECB or CBC or CBC-MAC or GCM or OFM or CBC) w/10 meeting	7,823	1,395
6	(encipher or decipher or decrypt) w/10 meeting	17, 867	1,487

Zoom has agreed to employ terms 1 and 2 (as the "green shield" in the Zoom App is related to end-to-end encryption). Because term 3 generated a high number of documents, Zoom proposes modifying the term to (stor* w/3 key*) w/10 meeting, which would target the storage of encryption keys for meeting data and thus exclude discussion of key storage for other purposes. This generates 516 document hits including family members.

Zoom cannot agree to use search terms 4, 5 and 6, all of which have nothing to do with the end-to-end nature (or lack thereof) of Zoom's encryption—as opposed to other features of its encryption. Thus, these terms are likely to return high numbers of irrelevant documents and would place a disproportionate burden on Zoom. Search term 4 refers to AES, which concerns the type (or strength) of encryption used, not whether the system was end-to-end or not. Similarly, search term 5 refers to specific means by which encryption can be applied to data and transmissions of data, not whether the encryption implementation is end-to-end or not. Search term 6 likewise does not pertain to the end-to-end nature of encryption (or lack thereof), but is generically about encryption and decryption of data.

Respectfully submitted,

Dated: February 18, 2021

/s/ Tyson Redenbarger
Tyson Redenbarger
tredenbarger@cpmlegal.com
COTCHETT, PITRE & MCCARTHY, LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577

Tina Wolfson
twolfson@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, California 91505
Tel: (310) 474-9111
Fax: (310) 474-8585

Interim Co-Lead Counsel for Plaintiffs

Dated: February 18, 2021

/s/ Kathleen Hartnett
Kathleen R. Hartnett
(khartnett@cooley.com)

COOLEY LLP
101 California Street, 5th Floor
San Francisco, California 94111-5800
Telephone: +1 415 693 2000
Facsimile: +1 415 693 2222

Counsel for Defendant Zoom Video Communications, Inc.

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)

I, Tyson C. Redenbarger, attest that concurrence in the filing of this document has been obtained from the other signatory. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 18th day of February 2021, at Burlingame, California.

/s/ Tyson C. Redenbarger
Tyson C. Redenbarger